UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,670	01/16/2002	Michael Raley	111325-000200	2328

22204   7590   12/22/2008
NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER
DADA, BEEMNET W

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
12/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<table>
<tr><td rowspan="2">Office Action Summary</td><td>Application No.</td><td>Applicant(s)</td><td></td></tr>
<tr><td>10/046,670</td><td>RALEY ET AL.</td><td></td></tr>
<tr><td>Examiner</td><td>Art Unit</td><td></td></tr>
<tr><td>BEEMNET W. DADA</td><td>2435</td><td></td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>17 November 2008</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-79</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-79</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible

for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has

been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37

CFR 1.114. Applicant's submission filed on November 17, 2008 has been entered. Claims 1

and 37 have been amended. Claims 1-79 are pending.

Response to Arguments

Applicant's arguments, with respect to 35 USC 112 1st paragraph rejections of claims 77

and 79 have been fully considered and are persuasive. The rejections of claims 77 and 79

under 35 USC 112 1st paragraph has been withdrawn.

Applicant's arguments with respect to 35 USC 103(a) rejections have been fully

considered but they are not persuasive. Applicant argues that the Peinado patent fails to teach

a security module that selectively intercepts a request to the rendering engine to render the

digital content based upon the usage rights associated with the digital content as recited in

claim 1. Applicant further argues that the Rabin Patent fails to cure the deficiencies of the

Peinado patent. Examiner disagrees.

Examiner would point out that Peinado teaches client side security module, separate

from the rendering engine, which is downloaded and included in said client computer, the

security module being adapted to be attached to the standard application program for enforcing

security conditions for accessing the rendering engine [column 3, lines 33-67, figure 4, DRM

system 32, Black Box 30 and column 13, lines 20-31]. Wherein the security module determines

if the requested digital content is protected content based upon the usage rights associated with

the requested digital content [column 15, lines 6-20], and wherein if the security module

determines that the requested digital content is protected content, the security module

determines whether to allow a user to perform a requested function on the protected content

based upon the usage rights associated with the protected digital content, and responds to the

request to perform the requested function on the protected digital content based on the usage

rights associated with the protected digital content [column 15, lines 10-51 and column 16, lines

55-65] as indicated in the rejection of claim 1 below. Furthermore, Rabin teaches a security

module, that determines if the requested digital content is protected content based upon the

usage rights associated with the requested digital content and if the requested digital content is

protected content the security module intercepts requests to a rendering engine to render the

digital content that would enact a violation of usage rights associated with the content [see

Rabin, column 11, lines 9-34 and column 24, lines 33-48]. Examiner would point out that the art

on record teaches the claim limitations and therefore the rejection is respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-23, 26-34, 36-59, 62-70, 72 and 76-79 are rejected under 35 U.S.C. 103(a) as
being unpatentable over Peinado et al. US Patent 6,816,596 (hereinafter Peinado) in view of
Rabin et al. US 6,697,948 B1 (hereinafter Rabin).

As per claim 1, Peinado teaches a system for distributing digital documents having
usage rights associated therewith, said system comprising:

a server having at least one digital document stored thereon [column 2, lines 60-67]

a client computer having a standard application program including a rendering engine
capable of being accessed to render content [column 3, lines 5-13, figure 4, units 34 and
column 15, lines 6-10];

a communications network coupled to said client and said server [column 2, lines 61-67];
and

a client side security module, separate from the rendering engine, which is downloaded
and included in said client computer, the security module being adapted to be attached to the
standard application program for enforcing security conditions for accessing the rendering
engine [column 3, lines 33-67, figure 4, DRM system 32, Black Box 30 and column 13, lines 20-
31].

Wherein the security module determines if the requested digital content is protected
content based upon the usage rights associated with the requested digital content [column 15,
lines 6-20], and

wherein if the security module determines that the requested digital content is protected
content, the security module determines whether to allow a user to perform a requested function
on the protected content based upon the usage rights associated with the protected digital
content, and responds to the request to perform the requested function on the protected digital

content based on the usage rights associated with the protected digital content [column 15, lines 10-51 and column 16, lines 55-65]; and

wherein if the security module determines that the requested digital content is not protected content, the security module disengages from the rendering engine [column 15, lines 1-5].

Peinado further teaches the system determining if a request for digital content is for protected content and granting of denying access to the content based on usage rights associated with the content only if it is determined by the security module that the requested digital content is protected content [figure 5B, steps 503-507, 517, column 14, line 66-column 15, line 19].

Peinado is silent on the system, wherein the security module intercepts requests to the rendering engine. However, within the same field of endeavor, Rabin teaches a system for protecting information, including a security module, that determines if the requested digital content is protected content based upon the usage rights associated with the requested digital content and if the requested digital content is protected content the security module intercepts requests to a rendering engine to render the digital content that would enact a violation of usage rights associated with the content [see Rabin, column 11, lines 9-34 and column 24, lines 33-48], and thus grant or denies the request to access the content based on the usage rights associated with the content (i.e., determining the use policy of a tag associated with the instance software, and determining if the request is valid by examining the tag/tag table (usage supervision/rights) and allowing/denying access, see figure 8, steps 275, 276, column 18, lines 10-29). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Rabin within the system of Peinado in order to further enhance security of the system.

As per claims 2 and 3, Peinado further teaches the system wherein the security
conditions include usage rights associated with the content [column 3, lines 45-56].

As per claims 4, 23 and 36, Peinado further teaches wherein said security module is
operative to determine if said client computer is missing any security component software based
on a predetermined configuration required for managing security of requested content and if
said at least one client unit is missing any security component software based on said
predetermined configuration, said security module is operative to provide said missing security
component software to said client computer [column 15, lines 25-50].

As per claims 5, Peinado further teaches the system wherein if said security module
determines that the request is not for protected content, the security module deactivates
[column 35 line 66 – column 36 line 18].

As per claim 6, Peinado further teaches the system wherein said server comprises plural
server computers and said security module is operative to cause said client computer to
exchange one or more keys with a first of said server computers to obtain a validation
certificate, said validation certificate permitting said client computer to securely communicate
with a second of said server computers without any further exchange of keys between said
client computer and any of said server computers [column 3, lines 5-23].

As per claims 7 and 8, Peinado teaches the system wherein said security module is
operative to define a user interface of said standard application in accordance with parameters
specified by said server [column 14, lines 16-34].

As per claims 9-11, Peinado teaches the system wherein said security module is
operative to superimpose a watermark based on client specific data on a image rendered by
said rendering engine [column 8, lines 3-13].

As per claims 12-17, 26-27, 32-34 Peinado teaches the system further comprising a transaction aggregator system for managing transactions relating to document distribution and a server side security component that directs the client computer to the transaction aggregator to receive a client side security component in exchange for transmitting user information to the transaction aggregator when said client computer makes a request for content and when said client side security component is not installed in said client computer, and wherein said transaction aggregator validates said client computer, based on predetermined conditions, and wherein said client side security component is unique to thereby identify said client computer to said server and to permit said server to report information relating to transactions with said client side computer to said transaction aggregator [column 15, line 58 – column 16, line 15].

As per claim 18-19, Peinado teaches the system wherein said server comprises a storage device containing a folder of embedded links to digital content and wherein the address of said folder is selected one of and to be difficult to ascertain, said security module being operative to provide information relating to at least one of the links when said client computer sends a request for content to said server and said security module indicates that that said client computer is authorized to access the content [column 2, line 64 – column 3, line 13].

As per claims 20-22, Peinado further teaches the system wherein said security module creates a document containing references to the digital content and spawns a child instance of the rendering engine to render the document, and wherein said child instance of said rendering engine is operative to follow the references to retrieve content through an asynchronous protocol from a secured location [column 13, line 59 – column 14, line 16].

As per claims 28 and 29, Peinado further teaches the system wherein said security component embeds all security information in a header of a document transmitted between said

client computer and said server, said document having a body that does not contain security information for content in the document [column 19, lines 47-60].

As per claim 30 and 31, Peinddo further teaches the system wherein said security module is operative to check a request made by said client computer at two stages, a first stage filter checks if said request corresponds to a prohibited URL and a second stage filter checks if said request corresponds to a prohibited directory, and wherein if said request corresponds to a prohibited URL, or if said request corresponds to a prohibited directory, then said request is denied by said server [column 17, lines 12-37].

As per claims 76, Peinado further teaches the system wherein the security module is installed on the client computer separately from the standard application program [column 3, lines 33-67].

As per claims 77, Peinado further teaches the system wherein the security module is installed on the client computer at a different time than the standard application program [column 3, lines 33-67].

As per claims 37-59, 62-70, 72, 78 and 79, the claimed steps correspond to the functions of the elements of the system claims 1-36, 76 and 77 which has been rejected above and thus rejected with the same reason.

Claims 73-75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peinado et al. US Patent 6,816,596 (hereinafter Peinado) in view of Rabin et al. US 6,697,948 B1 (hereinafter Rabin) and further in view of Luckenbaugh et al. US 6,311,269 B2 (hereinafter Luckenbaugh).

As per claims 73-75, the combination of Peinado and Rabin teaches the claim limitations as indicated above. Peinado and Rabin teach delivering content, intercepting a security information and honoring usage rights while processing the content as indicated above.

Peinado-Rabin is silent on the system wherein an HTML header and body, including security information embedded as recited in claims 73-75. However, within the same field of endeavor, Luckenbaugh teaches an HTML document adapted to be rendered by Web browser in a secure environment (figure 2B), said document comprising: an HTML header defined between header tags (figure 2B, step 233); an HTML body containing content (figure 2B, step 234); and security information (i.e., Cookie) embedded in said header, said security information being associated with one or more usage rights [figure 2B, step 233 and column 8, line 53 – column 9, line 16]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Luckenbaugh within the combination of Peinado and Rabin in order to render content in an HTML based environment and provide efficient access to content.

Allowable Subject Matter

Claims 24, 25, 35, 60, 61 and 71 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/
Examiner, Art Unit 2435
December 18, 2008